

Сравнение по модулю идеала

- Пусть K — коммутативное кольцо, I — идеал в K .

Коммутативное кольцо:

- 1) Ассоциативность $+$
- 2) Коммутативность $+$
- 3) Ноль
- 4) Обратный элемент по $+$
- 5) Дистрибутивность
- 6) Ассоциативность $*$
- 7) Коммутативность $*$

Идеал:

I подкольцо K ($I \subset K$, одни и те же операции $+$ и $*$) и выполнено: $\forall x \in K$ и $\forall a \in I$: $ax \in I$, то есть при “перемножении” любого элемента из идеала на любой элемент из кольца, мы остаёмся в пределах идеала.

Определение

Пусть $a, b \in K$. Тогда $a \equiv_I b$ (или, что то же самое, $a \equiv b \pmod{I}$), если и только если $a - b \in I$.

Лемма 10

\equiv_I — отношение эквивалентности (то есть, рефлексивно, симметрично и транзитивно).

Доказательство. • $a \equiv_I a$, так как $a - a = 0 \in I$.

• Если $a \equiv_I b$, то $a - b \in I$. Значит, $b - a \in I$, откуда $b \equiv_I a$.

• Если $a \equiv_I b$ и $b \equiv_I c$, то $a - b, b - c \in I$. Значит, $a - c = (a - b) + (b - c) \in I$, откуда $a \equiv_I c$. □

(Рефлексивность: xRx выполнено для $\forall x \in X$)

Симметричность: из xRy следует yRx

Транзитивность: из xRy и yRz следует xRz)

Комментарии к доказательству: 0 лежит в кольце по определению; в кольце по определению лежит обратный элемент; кольцо по определению замкнуто по сложению

Определение

Вычет по модулю идеала I — это класс эквивалентности по \equiv_I .

- Различные вычеты не пересекаются. Кольцо K разбито на вычеты.

То есть все элементы кольца разбиваются по кучкам (классам) и для каждой кучки (класса) находится такое I , что выполнено определение отношения эквивалентности для любых двух элементов из кучки.

Факторкольцо

- Для $a \in K$ вычет, состоящий из элементов кольца, сравнимых с a , как правило, будем обозначать через \bar{a} .
- Из определения следует, что $\bar{a} = a + I = \{a + x : x \in I\}$.

Определение

- Пусть K — коммутативное кольцо, I — идеал в K .

Факторкольцо $K/I := \{\bar{a} : a \in K\}$.

- $\bar{a} + \bar{b} := \overline{a + b}; \quad \bar{a} \cdot \bar{b} := \overline{ab}$.

Лемма 11

$+$ и \cdot в K/I определены корректно.

Доказательство. • Пусть $a \equiv_I a'$, то есть, $\bar{a} = \bar{a}'$. Это означает, что $a - a' \in I$. Докажем, что от замены a на a' результат $+$ и \cdot не изменится:

$$\bar{a} + \bar{b} = \bar{a}' + \bar{b} \iff a + b \equiv_I a' + b \iff a + b - (a' + b) = a - a' \in I;$$

$$\bar{a} \cdot \bar{b} = \bar{a}' \cdot \bar{b} \iff ab \equiv_I a'b \iff$$

$$ab - (a'b) = (a - a')b \in I \iff a - a' \in I. \quad \square$$

Комментарии к доказательству: a и a' сравнимы по модулю I и $\bar{a} = \bar{a}'$ это просто одна и та же запись. Потом добавили \bar{b} к обеим частям равенства. Далее сказали, что $\bar{a} + \bar{b} = \overline{a + b}$, аналогично $\bar{a}' + \bar{b} = \overline{a' + b}$ (это факторкольцо)

Теорема 1

- K/I с определенными выше $+$ и \cdot — коммутативное кольцо.
- Если K — кольцо с 1, то K/I — тоже. Если при этом $a \in K$ — обратимый элемент в K , то \bar{a} — обратимый в K/I .

Доказательство. • Так как $\bar{a} + \bar{b} = \overline{a + b}$, из ассоциативности и коммутативности $+$ в K следует ассоциативность и коммутативность $+$ в K/I .

• Так как $\bar{a} \cdot \bar{b} = \overline{ab}$, из ассоциативности и коммутативности умножения в K следует ассоциативность и коммутативность умножения в K/I .

• **Дистрибутивность:**

$$\bar{a}(\bar{b} + \bar{c}) = \overline{a(b + c)} = \overline{ab + ac} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}.$$

• **Ноль** — это $\bar{0}$.

• **Обратный по сложению:** $-\bar{a} := \overline{-a}$.

• **Единица:** если $1 \in K$, то $\bar{1}$ — единица в K/I .

• Если $a \in K$ — обратимый, то $(\bar{a})^{-1} := \overline{a^{-1}}$ — обратный в K/I . □

Для коммутативного кольца:

- 1) Ассоциативность $+$ $(a+b)+c = a+(b+c)$, $\bar{a} = a + I$
- 2) Коммутативность $+$ $a+b = b+a$ $a+I+b+I = b+I+a+I$
- 3) Ноль
- 4) Обратный элемент по $+$
- 5) Дистрибутивность
- 6) Ассоциативность $*$ $((a+I)(b+I))(c+I) = (ab + I)(c+I) = abc + I$ аналогично с другой расстановкой скобочек
- 7) Коммутативность $*$ $ab = ba$ $(a+I)(b+I) = ab+I$
 $(b+I)(a+I) = ba + I$